КІБЕРБЕЗПЕКА

ISSN 2707-1898 (print)

Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2022.01.053
Article received 06.05.2022 p.
Article accepted 19.05.20221 p.
UDK 004.94

Correspondence author
I. G. Tsmots
ivan.tsmots@gmail.com

І. Г. Цмоць, Ю. В. Опотяк, О. Я. Різник, О. М. Березький, Ю. А. Лукащук
Національний університет "Львівська політехніка", м. Львів, Україна

АРХІТЕКТУРА ТА РЕАЛІЗАЦІЯ БАЗОВИХ КОМПОНЕНТІВ СИСТЕМИ НЕЙРОМЕРЕЖЕВОГО ЗАХИСТУ І КОДУВАННЯ ПЕРЕДАЧІ ДАНИХ

Описано розробку базових компонентів системи нейромережевого захисту, кодування передачі даних на основі інтегрованого підходу, який містить удосконалений метод нейромережевого шифрування (дешифрування) даних і метод адаптивного баркереподібного кодування (декодування) даних, які орієнтовані на сучасну елементну базу. Для розробки системи обрано принципи спеціалізації та адаптації апаратно-програмних засобів до структури алгоритмів нейроподібного шифрування (дешифрування) даних, архітектури нейромережі та розрядності баркереподібного коду. Запропоновано архітектуру системи, що враховує змінний склад обладнання та модульність. Вдосконалено метод нейромережевого шифрування (дешифрування) даних, який внаслідок розпаралелення процесу шифрування (дешифрування) та використання таблиць макрочасткових добутків забезпечує зменшення часу шифрування (дешифрування) при програмній реалізації. Розроблено метод адаптивного баркереподібного кодування / декодування, який внаслідок врахування співвідношення сигнал/шум забезпечує високу завадостійкість та зменшує час передачі даних. Описано апаратні засоби системи, яку створено з використанням розроблених базових компонентів нейромережевого захисту та баркереподібного кодування даних. З використанням створеної системи визначено, що виконання операцій нейромережевого криптографічного шифрування (дешифрування) блоків даних на базі мікрокомп'ютера здійснюється у часі, близькому до реального. Час формування і навчання нейромережі становить біля 200 мс, а виконання процедур шифрування та дешифрування становить відповідно біля 35 мс та 30 мс і не залежить істотно від обраної конфігурації нейроподібної мережі.

Ключові слова: криптографічний захист; архітектура мобільної системи; бортові засоби; метод нейромережевого шифрування (дешифрування) даних; метод адаптивного баркереподібного кодування / декодування.

Вступ/Introduction

При дистанційному управлінні рухом мобільних робототехнічних платформ важливою проблемою є забезпечення надійного зв'язку між такими платформами та віддаленим центром керування з забезпеченням відповідного рівня криптографічного захисту та завадостійкості з одночасним зменшенням маси, габаритів, енергоспоживання та вартості засобів для їх реалізації. Розроблення мобільних бортових засобів криптографічного захисту та завадостійкого кодування з високими техніко-економічними показниками вимагає широкого використання сучасної елементної бази, розроблення нових методів, алгоритмів і структур, орієнтованих на ефективну програмно-апаратну реалізацію алгоритмів шифрування-дешифрування та кодування-декодування даних. Одним із шляхів досягнення високих техніко-експлуатаційних характеристик є використання для криптографічного захисту нейроподібних мереж прямого поширення автоасоціативного типу, які навчаються неітеративним методом послідовних геометричних перетворень. Особливістю таких нейроподібних мереж є принципова можливість неітеративного обчислення вагових коефіцієнтів синаптичних зав'язків між нейронними елементами. Використання наперед обчислених вагових коефіцієнтів дає змогу зменшити час шифрування (дешифрування) даних.

Забезпечення високої завадостійкості та скритності передачі даних можна досягнути завдяки використанню баркереподібних кодів і засобів адаптації їх розрядності до величини завад. У зв'язку з цим актуальною проблемою є розроблення системи нейроподібного захисту, баркереподібного кодування та передачі даних з високими техніко-експлуатаційними параметрами, орієнтованої на використання у бортових системах.

Об'єкт дослідження – процеси нейромережевого шифрування / дешифрування, кодування / декодування та передачі даних.

Предмет дослідження – архітектура системи нейроподібного захисту, баркереподібного кодування та передачі даних, методи, алгоритми і засоби реалізації базових компонентів.

Мета роботи – розроблення архітектури та базових компонентів системи нейромережевого захисту, адаптивного баркероподібного кодування та передачі даних для застосування серед іншого і у вбудованих системах.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- аналіз останніх досліджень та публікацій;
- вибір підходу та принципів розробки системи нейромережевого захисту, баркероподібного кодування та передачі даних;
- розроблення структур стаціонарної та мобільної частин системи нейромережевого захисту, баркероподібного кодування та передачі даних;
- програмна реалізація компонентів системи нейромережевого захисту, баркероподібного кодування та передачі даних;
- розроблення апаратних засобів системи нейромережевого захисту, баркероподібного кодування та передачі даних;
- тестування та оцінювання параметрів розроблених компонентів.

Аналіз останніх досліджень та публікацій. Аналіз основних тенденцій розвитку мобільних бортових систем криптографічного захисту даних показує, що для виконання шифрування та дешифрування даних у таких системах все більше використовуються нейромережеві методи [6], [9] , [11]. Аналіз публікацій [8], [16] показує, що наявні методи криптографічного захисту не орієнтовані на їх використання для побудови мобільних бортових систем криптографічного захисту даних.

У роботах [22], [23], розглянуто автоасоціативну нейронну мережу з неітераційним навчанням і шляхи її адаптації до задач криптографічного захисту даних. Показано, що особливістю такої нейромережі є можливість попереднього обчислення вагових коефіцієнтів. В роботі [7] описано використання методу головних компонент для попереднього обчислення вагових коефіцієнтів. Метод головних компонент використовує систему власних векторів, які відповідають власним значенням коваріаційної матриці вхідних даних [4].

У роботах [12], [17], [22] окреслено особливості використання автоасоціативної нейромережі з наперед обчисленими ваговими коефіцієнтами для задач криптографічного шифрування та дешифрування даних. Для нейромережевого криптографічного шифрування та дешифрування даних у роботі [28] запропоновано використовувати коди маскування, архітектуру нейромережі та матриці вагових коефіцієнтів у якості ключів.

У роботах [19], [26], [27] розглянуто методи синтезу баркероподібних послідовностей та алгоритми завадостійкого кодування / декодування з використанням баркероподібних кодів. Недоліком розглянутих методів є відсутність можливості адаптації розрядності баркероподібних кодів до величини завад.

З аналізу робіт [20], [25] видно, що нейромережеві засоби криптографічного симетричного шифрування та дешифрування даних реалізуються на базі обчислювального ядра, доповненого апаратними засобами, які реалізують складні обчислювальні операції. Висока швидкодія нейромережевих засобів криптографічного шифрування та дешифрування даних досягається завдяки розпаралеленню та використанню таблично-алгоритмічних методів реалізації операцій обчислення скалярного добутку. Недоліком наявних нейромережевих засобів криптографічного захисту даних є невисока швидкодія.

Результати дослідження та їх обговорення / Research results and their discussion

Розроблення архітектури системи нейромережевого захисту та баркероподібного кодування передачі даних. Вибір підходу та принципів розробки. Розроблення апаратних і програмних засобів системи нейромережевого захисту, баркероподібного кодування передачі даних між віддаленим центром управління та мобільною робототехнічною платформою пропонується здійснювати з використанням інтегрованого підходу, який охоплює вдосконалення методу нейромережевого шифрування (дешифрування) даних і методу адаптивного баркероподібного кодування / декодування з орієнтацією на застосування сучасної елементної бази.

Розроблення апаратних і програмних засобів системи нейромережевого захисту, баркероподібного кодування та передачі даних між віддаленим центром управління та мобільною робототехнічною платформою базується на використанні принципів:

- змінного складу обладнання, що передбачає наявність процесорного ядра та змінних модулів, за допомогою яких ядро адаптується до вимог конкретного застосування;
- модульності, який передбачає розробку компонентів системи у вигляді функціонально завершених пристроїв;
- відкритості програмного забезпечення, що передбачає можливості нарощування та його вдосконалення, максимального використанням стандартних драйверів та програмних засобів;
- спеціалізації і адаптації апаратно-програмних засобів до структури алгоритмів нейромережевого шифрування (дешифрування), баркероподібного кодування (декодування) даних;
- програмної зміни архітектури нейромережі та розрядності баркероподібного коду.

Ефективність системи нейромережевого захисту даних, баркероподібного кодування передачі даних безпосередньо пов'язана з вибором програмно-апаратних засобів реалізації. Програмна реалізація системи нейромережевого захисту, баркероподібного кодування передачі даних передбачає використання мікропроцесорів і мікроконтролерів. При програмній реалізації нейромережевих алгоритмів шифрування та дешифрування даних обчислювальні процеси переважно розгортаються в часі з великим об'ємом пересилання інформації між оперативною пам'яттю і операційними пристроями. Програмні засоби при цьому вимагають розв'язання задачі мінімізації об'єму програм і часу їх реалізації при заданій точності обчислень. Причому, вказані засоби характеризуються високою гнучкістю з точки зору можливості модифікації та зміни алгоритмів і низькою швидкодією.

Переваги інтегральних технологій забезпечують широке використання апаратної реалізації нейроподібних алгоритмів. При такій реалізації процес обчислення розгортається як у часі, так і в просторі. Апаратна реалізація характеризуються введенням додаткового обладнання і відсутністю проміжних пересилань інформації в процесі обчислення, а також спрощенням функції місцевого управління. В основі структурної організації апаратних засобів лежить принцип адекватного апарат-

ного відображення алгоритмів нейромережевого шифрування (дешифрування) та баркероподібного кодування (декодування) даних.

Потрібно відзначити, що тільки програмна або апаратна реалізація алгоритмів нейромережевого шифрування (дешифрування) та баркероподібного кодування (декодування) даних на практиці трапляється нечасто. В більшості випадків для реалізації таких алгоритмів використовується процесорне ядро, доповнене апаратними засобами, які реалізуються на базі програмованих логічних інтегральних схем (ПЛІС).

Розроблення структури стаціонарної частини системи нейромережевого захисту та баркероподібного кодування передачі даних. Задача розробки системи нейромережевого захисту з високими техніко-експлуатаційними характеристиками зводиться до мінімізації апаратних затрат при забезпеченні множини вимог і обмежень. Вона реалізується за принципами змінного складу обладнання та модульності. Система нейромережевого захисту, баркероподібного кодування та передачі даних складається зі стаціонарної частини, яка є віддаленим центром керування та мобільної частини, яка розміщена на робототехнічній платформі. Структура стаціонарної частини системи нейромережевого захисту, баркероподібного кодування передачі даних наведена на рис. 1,*a*.

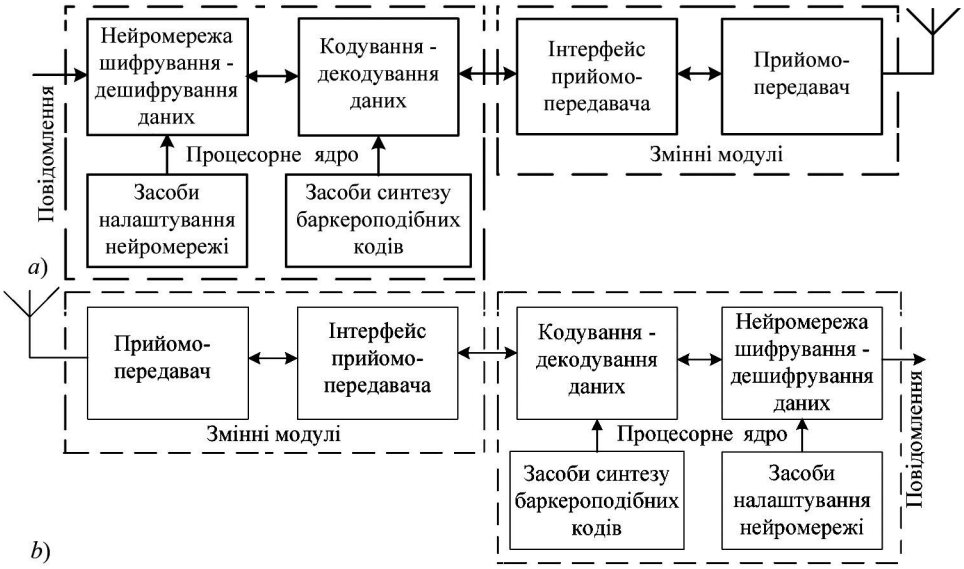

Рис. 1. Структура системи нейромережевого захисту та баркероподібного кодування передачі даних: *a*) стаціонарної частини; *b*) мобільної частини / The structure of the system of neural network protection and barque-like coding of data transmission: *a*) stationary part; *b*) mobile part

Обчислювальне ядро центру керування може бути реалізоване на базі персонального комп'ютера (ноутбука), наприклад, з архітектурою процесора Intel IA-64. У вигляді програмних модулів реалізується інтерфейсна частина для взаємодії з оператором з метою керування об'єктом, який отримує шифровані команди і дані та декодує їх за допомогою мобільної частини системи нейромережевого захисту, баркероподібного кодування та передачі даних. Для фізичної передачі радіоканалом зашифрованих даних використовується прийомо-передавач, який зв'язується з обчислювальним ядром за допомогою стандартних інтерфейсів, та керується мікроконтролером.

Розроблення структури мобільної частини системи нейромережевого захисту та баркероподібного кодування передачі даних. Мобільна частина системи нейромережевого захисту, баркероподібного кодування та передачі даних реалізується на базі процесорного ядра, яке при необхідності може бути доповнене спеціалізованими апаратно-програмними засобами. Процесорне ядро мобільної частини системи нейромережевого захисту, баркероподібного кодування передачі даних реалізується на базі сучасного мікрокомп'ютера. Структура мобільної частини системи нейромережевого захисту, баркероподібного кодування та передачі даних наведена на рис. 1,*b*.

Основними компонентами мобільної частини системи нейромережевого захисту, баркероподібного кодування передачі даних є: прийомо-передавач, інтерфейс прийомо-передавача, засоби синтезу баркероподібних кодів, засоби кодування-декодування, нейромережа для шифрування та дешифрування даних, засоби налаштування нейромережі. Мобільна частина системи реалізується на базі сучасної елементної бази (мікрокомп'ютерів, мікроконтролерів) з поєднанням універсального та спеціалізованого підходів, програмних і апаратних засобів, що забезпечує реалізацію вимог, які висуваються до маси, габаритів і енергоспоживання.

Удосконалення нейромережевого шифрування та дешифрування даних. Навчання нейронної мережі полягає в попередньому обчислені матриці вагових коефіцієнтів W, яка утворюється з власних векторів автоковаріаційної матриці вхідних даних R. Нейромережеве шифрування даних зводиться до множення обчисленої матриці вагових коефіцієнтів W на вектор вхідних даних $\bar{x}$ відповідно з наступною формулою:

$$y_j = \begin{vmatrix} W_{11} & W_{12} & \cdots & W_{1k} \\ W_{21} & W_{22} & \cdots & W_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ W_{N1} & W_{N2} & \cdots & W_{Nk} \end{vmatrix} \times \begin{matrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{matrix}. \quad (1)$$

Множення матриці вагових коефіцієнтів W на вектор вхідних даних $\bar{x}$ зводиться до виконання N операцій обчислення скалярного добутку:

$$y_j = \sum_{s=1}^{k} W_{js} x_s, \quad (2)$$

де k – кількість добутків, $s = 1,2,\ldots,k$, $j = 1,2,\ldots,N$.

Для дешифрування зашифрованих даних необхідно із обчисленої матриці вагових коефіцієнтів W шляхом її транспонування сформувати транспоновану матрицю вагових коефіцієнтів:

$$\begin{vmatrix} W_{11} & W_{12} & \cdots & W_{1k} \\ W_{21} & W_{22} & \cdots & W_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ W_{N1} & W_{N2} & \cdots & W_{Nk} \end{vmatrix}^T = \begin{vmatrix} W_{11} & W_{21} & \cdots & W_{N1} \\ W_{12} & W_{22} & \cdots & W_{N2} \\ \vdots & \vdots & \cdots & \vdots \\ W_{1k} & W_{2k} & \cdots & W_{Nk} \end{vmatrix}. \qquad (3)$$

Нейромережеве дешифрування зашифрованих даних зводиться до множення транспонованої матриці вагових коефіцієнтів W^T на вектор зашифрованих даних $\bar{y}$ відповідно з наступною формулою:

$$x_s = \begin{vmatrix} W_{11} & W_{21} & \cdots & W_{N1} \\ W_{12} & W_{22} & \cdots & W_{N2} \\ \vdots & \vdots & \cdots & \vdots \\ W_{1k} & W_{2k} & \cdots & W_{Nk} \end{vmatrix} \times \begin{matrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{matrix}. \qquad (4)$$

Множення транспонованої матриці вагових коефіцієнтів W^T на вектор зашифрованих даних $\bar{y}$ зводиться до виконання N операцій обчислення скалярного добутку:

$$x_s = \sum_{j=1}^{N} W_{sj} y_j \,, \qquad (5)$$

де N – кількість добутків, $s = 1,2,\ldots,k$, $j = 1,2,\ldots,N$.

Для програмної реалізації скалярного добутку доцільно використовувати алгоритм множення з аналізом одного розряду множника. Ґрунтуючись на такому алгоритмі множення розробляється алгоритм обчислення скалярного добутку, який зводиться до інтегральної макрооперації групового підсумовування:

$$\begin{aligned} Z &= \sum_{j=1}^{N} W_j X_j = \sum_{j=1}^{N} \sum_{i=0}^{n-1} (-1)^{2^{-i}} 2^{-i} W_j x_{ji} = \\ &= \sum_{j=1}^{N} \sum_{i=0}^{n-1} (-1)^{2^{-i}} 2^{-i} P_{ji} = \sum_{i=1}^{n} (-1)^{2^{-i}} 2^{-i} P_{Mi}, \end{aligned} \qquad (6)$$

де $P_{Mi} = \sum_{j-1}^{N} P_{ji}$.

При обчисленні скалярного добутку за формулою (6), доцільно використовувати таблицю наперед обчислених макрочасткових добутків P_{Mi}. Формування макрочасткових добутків P_{Mi} на основі таблиці здійснюється за такою формулою:

$$P_{Mi} = \begin{cases} 0, \quad \text{якщо} \quad x_{1i} = x_{2i} = x_{3i} = \ldots = x_{mi} = 0; \\ W_1, \quad \text{якщо} \quad x_{1i} = 1, \quad x_{2i} = x_{3i} = \ldots = x_{mi} = 0; \\ W_2, \quad \text{якщо} \quad x_{1i} = 0, x_{2i} = 1, x_{3i} = \ldots = x_{mi} = 0; \\ W_1 + W_2, \quad \text{якщо} \quad x_{1i} = 1, x_{2i} = 1, x_{3i} = \ldots = x_{mi} = 0; \\ \vdots \\ W_1 + W_2 + \ldots + W_N, \text{ якщо } x_{1i} = 0, x_{2i} = x_{3i} = \ldots = x_{Ni} = 1; \\ W_1 + W_2 + \ldots + W_N, \text{якщо } x_{1i} = x_{2i} = x_{3i} = \ldots = x_{Ni} = 1. \end{cases} \qquad (7)$$

Обчислення скалярного добутку за формулами (6 і 7) зводить процес обчислення до заповнення, читання макрочасткових добутків P_{Mi} із таблиці та їх додавання до раніше накопичених сум відповідно з формулою:

$$Z_i = 2^{-1} Z_{i-1} + P_{Mi} \,, \qquad (8)$$

де $Z_0 = 0$.

При використанні програмних засобів для реалізації нейромережевого шифрування та дешифрування даних пропонується розпаралелити процес шифрування (дешифрування) та здійснювати вибір обсягів таблиць. Час нейромережевого шифрування та дешифрування даних залежить від розміру таблиць макрочасткових добутків P_{Mi} . Розмір таблиць наперед порахованих макрочасткових добутків P_{Mi} вибирається з умови забезпечення виконання шифрування та дешифрування даних у реальному часі.

Метод адаптивного баркереподібного кодування та декодування даних. Синтез баркереподібної кодової послідовності здійснюється шляхом використання унікальних властивостей "ідеальних кільцевих в'язанок" (ІКВ) – впорядкованість цілочислових послідовностей з кільцевою структурою, всі n чисел яких разом з усіма сумами поруч розміщених чисел R разів вичерпують натуральний ряд. Така багатопозиційна завадостійка кодова послідовність називається баркереподібним кодом. Для синтезу баркереподібного коду з довжиною кодових комбінацій S_n, за допомогою ІКВ достатньо виділити рядок із S_n пронумерованих позицій одновимірного масиву та заповнити одиницями ті позиції коду, номери яких збігаються з числом x_j, а інші заповнити нулями. Номери позицій коду, які збігаються з числом x_j знаходяться так:

$$x_j - 1 \equiv \sum_{i=1}^{j} k_i \left(\operatorname{mod} S_n\right), j = 1,2,...,n \,, \qquad (9)$$

$$S_n = n\left(n-1\right)/R + 1 \,, \qquad (10)$$

де k_i – i-ий елемент обраного ІКВ; n, R – параметри ІКВ.

Отримана послідовність двійкових символів є твірною комбінацією кодової послідовності, решта $S_n - 1$ кодових послідовностей формується циклічним зсувом. Мінімальну кодову відстань для сформованої кодової послідовності визначають так:

$$d_{\min} = 2(n - R) \,. \qquad (11)$$

За допомогою сформованої кодової послідовності, яка залежить від параметрів n і R можна виявити таку кількість помилок:

$$t_1 \le 2\left(n - R\right) - 1 \,. \qquad (12)$$

Залежно від параметрів n і R за допомогою сформованої кодової послідовності можна виправити наступну кількість помилок:

$$t_2 \le n - R - 1 \,. \qquad (13)$$

Використовуючи формули (9 і 10) синтезується баркереподібна кодова послідовність, яка використовується для кодування зашифрованих даних. Для кодування та декодування даних з використанням баркереподібних кодів розроблено метод, який забезпечує адаптацію довжини баркереподібного коду до величини завад. Кодування та декодування відповідно до пропонованого методу передбачає виконання наступних кроків:

Вибір довжини m і виду баркереподібного коду для кодування даних. Виконання порозрядного кодування зашифрованого числа починається із старшого розряду в такий спосіб: i-й розряд зашифрованого числа рівний лог.0 – передається баркереподібний код; i-й розряд зашифрованого числа рівний лог.1 – передається інверсне значення баркереподібного коду. Передача закодованого i-го розряду m розрядним баркереподібним кодом. Установлення вибраного баркереподібного коду розрядністю m для декодування даних.

Приймання i-го розряду закодованого m розрядним баркереподібним кодом. Виконання логічної операції

Виключне АБО над установленим *m* розрядним баркероподібним кодом і прийнятим *m* розрядним значенням *i*-го закодованого розряду. Формування результатів виконання логічної операції *Виключне АБО*: лог.0 (значення на входах одинакові), лог.1 (значення на входах різні). Підсумовування *m* результатів виконання логічної операції *Виключне АБО* і отримання суми $См_{ВикАБО}$.

Порівняння отриманої суми *См* із значенням (*m*+1)/2 та формування декодованого $i_д$-го розряду за наступною формулою:

$$i_д = \begin{cases} 0, & \text{коли} \quad См_{ВикАБО} < (m+1)/2 \\ 1, & \text{коли} \quad См_{ВикАБО} \geq (m+1)/2 \end{cases}. \qquad (14)$$

Визначення кількості розрядів $q_{пом}$ з помилками за такою формулою:

$$q_{пом} = \begin{cases} m - См_{ВикАБО}, & \text{коли} \quad i_д = 1 \\ См_{ВикАБО}, & \text{коли} \quad i_д = 0 \end{cases}. \qquad (15)$$

Аналіз $q_{пом}$ та прийняття рішення про зменшення чи збільшення довжини баркероподібного коду. Використання розробленого методу забезпечує високу завадостійкість та зменшує час передачі даних.

Реалізація базових компонентів системи нейромережевого захисту та баркероподібного кодування передачі даних. Програмна реалізація компонентів системи нейромережевого захисту, баркероподібного кодування та передачі даних передбачає використання обчислювальної потужності застосованих процесорних ядер. Програмні засоби модулів системи реалізовано на мові високого рівня С, що забезпечує програмну сумісність стаціонарної та мобільної частин системи, оскільки вони створюються і функціонують на різних апаратних платформах. Для створення програмних модулів стаціонарної частини у якості компілятора застосовується GCC/G++ та GDB debugger проекту MinGW-W64, а для мобільної при компіляції і відлагодженні – штатний компілятор GCC. Такий підхід дозволив проводити розробку та відлагодження програмних засобів з використанням персонального комп'ютера, а, при необхідності, виконувати доопрацювання модулів мобільної частини на базі мікрокомп'ютера.

Відлагодження розроблених модулів, об'єктивне тестування, виявлення та усунення помилок виконувалося незалежно один від одного. Далі вже розроблені і протестовані програмні модулі об'єднувалися у комплекс для забезпечення реалізації задач нейромережевого захисту, баркероподібного кодування (декодування) та передачі даних.

Комплекс програмного забезпечення системи нейромережевого захисту, баркероподібного кодування (декодування) та передачі даних містить такі програмні компоненти: нейромережевий шифратор, нейромережевий дешифратор, модуль їх налаштування, кодер з використанням баркероподібних кодів, декодер з використанням баркероподібних кодів, модуль синтезу баркероподібних кодів. Вказані програмні компоненти реалізуються за принципом відкритості програмного забезпечення, що передбачає можливості нарощування та автономного відлагодження. Для створення програмних компонентів використовується середовище розробки CodeBlocks, внаслідок доступності та вільного поширення.

Оскільки нейромережева технологія криптографічного захисту даних орієнтована на апаратно-програмну реалізацію, важливим етапом є оцінка швидкодії окремих компонентів та визначення компонентів, які є найбільш часомісткими. Комплекс реалізованих програмних модулів нейромережевого криптографічного шифрування / дешифрування даних містить наступні компоненти: Training_ANN, EnCrypt_ANN, DeCrypt_ ANN.

Основою комплексу є програмний засіб Training _ANN, що призначений для конфігурування і подальшого навчання нейроподібної мережі. Training_ANN застосовується однократно при виборі і заданні конфігурації мережі та забезпечує навчання конкретної реалізації нейроподібної мережі, що застосовується при шифруванні/дешифруванні даних. Вказаний програмний засіб виконує підготовку вхідних даних реалізації нейроподібної мережі відповідно до заданих значень вхідних параметрів, а саме: розрядності вхідних нейронів нейроподібної мережі; кількості нейронів вхідного шару нейроподібної мережі; кількості та розрядності навчальних векторів. На рис. 2 наведено вигляд інтерфейсу програми Training_ANN, за допомогою якого обираються вхідні параметри програмної реалізації нейроподібної мережі шифрування / дешифрування даних.

На основі заданих вхідних даних, які по суті є ключем для шифрування / дешифрування, обчислюються вагові коефіцієнти мережі для заданої архітектури. Результати виконання програми є даними для подальшого налаштування нейромережі як для шифрування даних на стаціонарній частині віддаленого центру управління, так і для налаштування нейромережі мобільної частини системи при дешифруванні.

Результати виконання розрахунків програмою записуються в файли, які власне і використовуються для налаштування нейромереж при роботі програм шифрування / дешифрування даних на стаціонарній та мобільній частинах системи.

На рис. 3 наведено вигляд робочого вікна середовища розробки CodeBlocks при створенні і відлагодженні програмних засобів. Як показують результати відлагодження програмного засобу Training_ANN час генерування всіх необхідних даних для конфігурації нейроподібної мережі та її навчання складає біля 400 мс. Варто зазначити, що власне вказаний процес конфігурації та навчання нейроподібної мережі потрібно проводити однократно.

Далі сконфігурована мережа застосовується для реалізації процесів нейромережевого шифрування / дешифрування даних. Програмний засіб EnCrypt_ANN шифрування даних на основі нейроподібної мережі використовує для своєї роботи файли налаштування, створені за допомогою Training_ANN. На основі даних з файлів налаштування конфігурується архітектура мережі (розрядність даних; розрядність вхідних нейронів нейроподібної мережі; кількість нейронів вхідного шару нейроподібної мережі) та вагові коефіцієнти для обраної архітектури. Далі у процесі роботи на вхід в такий спосіб сконфігурованої нейромережі подаються вхідні дані у вигляді вектора розрядністю *n*, а на виході нейромережі отримуємо зашифровані дані у форматі IEEE 754.

Програмний засіб DeCrypt_ANN, призначений для дешифрування даних на основі нейроподібної мережі, також використовує для роботи файли налаштування, створені за допомогою Training_ANN. Аналогічно задається архітектура мережі та вагові коефіцієнти і відбувається її функціонування у режимі дешифрування.

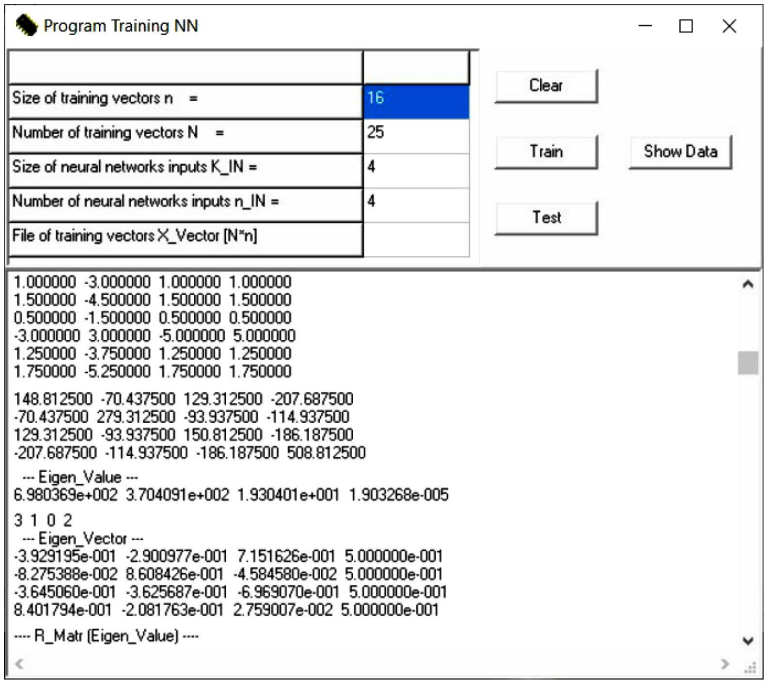

Рис. 2. Вигляд інтерфейсу програми Training_ANN / Appearance of the Training_ANN program interface

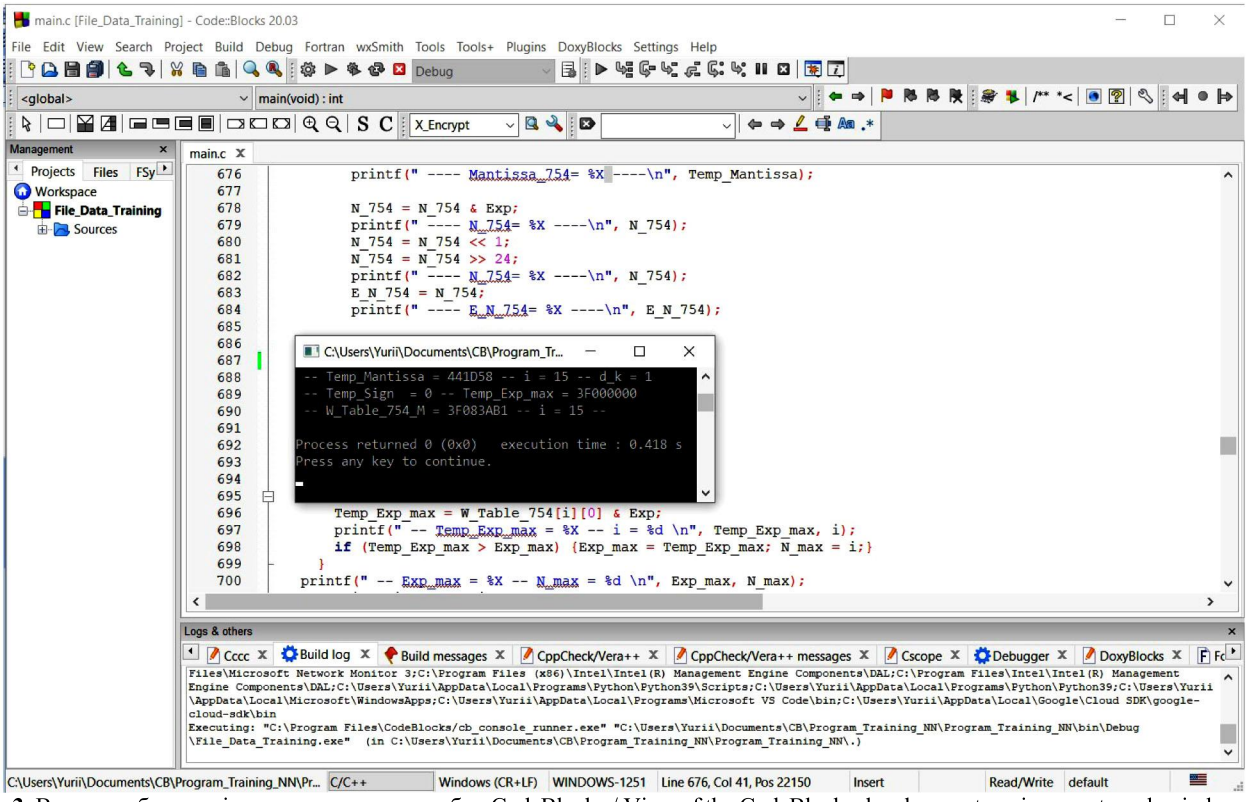

Рис. 3. Вигляд робочого вікна середовища розробки CodeBlocks / View of the CodeBlocks development environment work window

Розроблення апаратних засобів системи нейромережевого захисту та баркероподібного кодування передачі даних. Для передачі/прийому шифрованих/дешифрованих даних радіоканалом використовується зовнішній модуль прийомо-передавача, який зв'язується з ноутбуком за допомогою стандартного інтерфейсу USB та керується вбудованим мікроконтролером. Завданням мікроконтролера є отримання блоку даних з системи шифрування / дешифрування та, відповідно, передача/прийом його в ефір. При створенні апаратних засобів прийомо-передавача максимально використано готові компоненти та модулі промислового виробництва і брався до уваги рівень фізичної доступності апаратних компонентів на вітчизняному ринку, наявності відповідних засобів розробки програмного коду мікроконтролерів. Обраний мікроконтролер має у своєму складі відповідні апаратні інтерфейси для зв'язку з керуючим комп'ютером з використанням конвертора інтерфейсів USB – UART та для керування через інтерфейс, UART, I2C або SPI відповідно застосованого модуля трансивера. Завданням мікроконтролера є керування модулем трансивера та узгодження у процесі передачі (прийому) розмірів пакетів даних враховуючи технічні специфікації трансивера. Застосовано модуль трансивера

nRF24L01 з додатковим підсилювачем потужності типу E01-ML01DP5 фірми Ebyte. Модуль E01-ML01DP5 має підсилювач потужності, додатково повністю екранований та обладнаний виносною антеною. Такі переваги забезпечують більшу дальність передачі радіосигналу та вищу надійність прийому даних. У блоці прийомо-передавача системи зважаючи на вказані вимоги застосовано мікроконтролер на базі промислового модуля. Такий підхід забезпечив скорочення термінів розробки системи та належну якість реалізації апаратних засобів.

Макет розробленої стаціонарної частини системи нейромережевого захисту, баркероподібного кодування та передачі даних наведений на рис. 4.

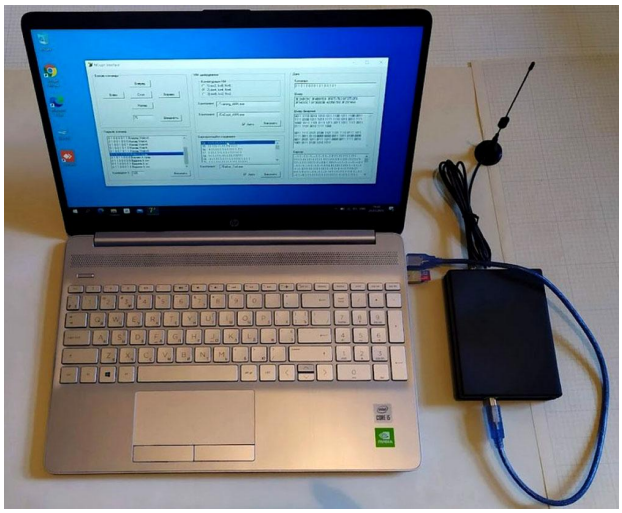

Рис. 4. Макет розробленої стаціонарної частини системи нейромережевого захисту та баркероподібного кодування передачі даних / Layout of the developed stationary part of the system of neural network protection and Barker-like coding of data transmission

З метою тестування радіоканалу в інших діапазонах частот та визначення впливу можливих завад у реальних умовах функціонування системи, внаслідок модульної конструкції, можливе застосування промислових модулів на основі трансиверів типу nRF24L01, SX1276, CC1101, SI4438/4463. Відпрацювання системного програмного забезпечення блоку інтерфейсу прийомо-передавача виконувалося за допомогою відкритого середовища розробки PlatformIO.

Засоби нейромережевого криптографічного шифрування / дешифрування даних мобільної частини системи реалізовано з використанням мікрокомп'ютера на базі SoC. Застосування мікрокомп'ютера забезпечує високу гнучкість щодо модифікації алгоритмів оброблення даних і достатню для реалізації вказаної задачі швидкодію. При створенні апаратних засобів мобільної частини системи також максимально застосовано готові компоненти та модулі промислового виробництва, що забезпечує адаптацію до конкретних умов застосування. Для реалізації необхідного функціоналу розроблено спеціальне програмне забезпечення і доповнено SoC необхідними зовнішніми модулями.

Застосування спеціалізованих дистрибутивів операційної системи Linux для функціонування мікрокомп'ютера передбачає використання штатних засобів розробки програмного забезпечення для них і, відповідно, стандартних компіляторів, включаючи GCC. Це, водночас, забезпечує переносимість програмного коду з однієї комп'ютерної платформи на іншу з мінімальною необхідністю його модифікації, яка, в основному, стосується взаємодії з пристроями вводу/виводу та з графічною підсистемою застосованого мікрокомп'ютера. Розроблені на мові високого рівня С програмні модулі блоків нейромережевого криптографічного шифрування / дешифрування, кодування / декодування були скомпільовані на обраній мікрокомп'ютерній платформі.

Для відпрацювання засобів нейромережевого криптографічного шифрування та дешифрування було застосовано не найпотужніший мікрокомп'ютер типу NanoPi Duo фірми FriendlyElec (FriendlyARM). NanoPi Duo розроблено для швидкого прототипування пристроїв, що забезпечує встановлення на макетні плати. Мікрокомп'ютер використовує SoC Cortex-A7 H2+ фірми Allwinner, містить 512МБ DDR3 оперативної пам'яті, вбудований модуль WiFi та має інтерфейси Ethernet, USB, SPI, UART, I2C, ШІМ. У якості ОС застосовується UbuntuCore.

Для спрощення взаємодії з мікрокомп'ютером при роботі з його файловою системою (копіювання, редагування тощо) було використано програмні засоби WinSCP на комп'ютері з ОС Windows, де виконується основне розроблення програмного забезпечення. При цьому, на персональному комп'ютері виконується редагування і базове тестування програмних засобів нейромережевого криптографічного шифрування та дешифрування даних, а далі, основні маніпуляції з файлами здійснюються засобами WinSCP. Компіляція та тестове виконання розроблених програмних засобів виконується на мікрокомп'ютері через консоль за допомогою програмного додатку PuTTY.

Розроблено макет для відпрацювання засобів нейромережевого криптографічного шифрування та дешифрування даних мобільної частини системи, який показано на рис. 5.

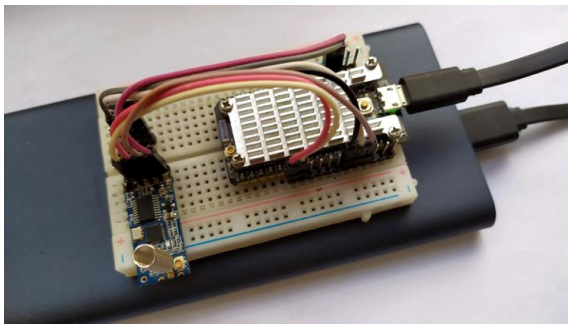

Рис. 5. Макет мобільного нейромережевого шифратора/дешифратора даних / Layout of neural network mobile data encoder/decoder

У макеті використано промисловий модуль прийомо-передавача типу HC-12, який містить власне трансивер Si4464 та керуючий мікроконтролер STM8C. Модуль забезпечує стандартний послідовний інтерфейс і безпосередньо під'єднаний до послідовного порту UART 1. Через послідовний порт UART 0 реалізується консоль керування мікрокомп'ютером. Варто зазначити, що його використовують при ініціалізації та встановленні ОС. Після цього консоль реалізується через бездротове з'єднання за допомогою програмного додатку PuTTY. Живлення макету здійснюється за допомогою портативного джерела живлення, яке має відповідний комп'ютерний роз'єм типу USB для забезпечення

під'єднання до мікрокомп'ютера за допомогою відповідного перехідника.

Тестування та оцінювання параметрів розроблених компонентів. Програмні засоби нейромережевого криптографічного шифрування та дешифрування розроблені з використанням мови С, що забезпечило їх кросплатформність. З метою тестування раніше розроблені і відлагоджені файли програм Training_ANN, EnCrypt_ANN, DeCrypt_ANN були скопійовані у файлову систему мікрокомп'ютера макету засобами WinSCP. Для їх компіляції було застосовано штатний компілятор GCC.

Після відлагодження програмних компонентів будо виконано оцінку часових затрат на виконання процесів нейромережевого криптографічного шифрування та дешифрування даних. Для цього застосовано штатну команду ОС *time* у наступному форматі

$$time./EnCrypt\_ANN > /dev/null$$

Тривалість виконання становив біля 35 мс. Аналогічно було протестовано тривалість виконання програмного модуля *DeCrypt_ANN* на мікрокомп'ютері, який становив біля 40 мс.

З метою тестування на мікрокомп'ютері було виконано тестування трьох варіантів архітектури нейроподібної мережі. Архітектура визначається кількістю нейроелементів *N,* кількістю входів *k* і їх розрядністю *m.* Від значення розрядності повідомлення *n* та кількості входів *k* залежить архітектура нейроподібної мережі. Для повідомлення розрядністю *n*=16 використано варіанти архітектури нейроподібної мережі у наступних конфігураціях:

- $m = 2, k = 8; N = 8;$
- $m = 4, k = 4; N = 4;$
- $m = 8, k = 2; N = 2.$

Далі виконувалося налаштування та навчання нейромереж і подальше виконання процесів шифрування / дешифрування для вказаних конфігурацій архітектури нейромереж. За результатами тестування було проведено оцінку часових параметрів, які наведено у табл. 1.

Табл. 1. Тривалість виконання процедури конфігурації/навчання, шифрування та дешифрування даних для обраних архітектур нейроподібної мережі / Configuration/training, encryption and decryption time for selected neural network architectures

Програмний засіб/Архітектура	$m = 2, k = 8;$ $N = 2$	$m = 4, k = 4;$ $N = 4$	$m = 8, k = 2;$ $N = 2$
Training_ANN, мс	189,7	197,4	203,2
EnCrypt_ANN, мс	37,2	29,3	37,8
DeCrypt_ANN, мс	38,4	22,9	24,9

Також було виконано оцінку температурного режиму роботи мобільної частини експериментальної системи на базі мікрокомп'ютера. Для оцінки динаміки зміни температури було використано скрипт, який у циклі виконував операції нейромережевого криптографічного шифрування та дешифрування. Отже, здійснювалося обчислювальне навантаження на мікрокомп'ютер. Скрипт виконувався тривалий час (30 хвилин). Аналіз показав, що при зростанні завантаженості процесора мікрокомп'ютера не відбувалося істотного підвищення його температури (очевидно, що цьому сприяє ефективний штатний радіатор). Отже, можна зробити висновок, що у процесі штатної експлуатації мобільної частини системи нейромережевого криптографічного шифрування та дешифрування даних проблем, пов'язаних з температурним режимом не повинно виникати.

Обговорення результатів дослідження. У роботах [1], [13], [14], [22], [24], [25] проаналізовано основні шляхи розвитку бортових засобів криптографічного захисту передачі даних у реальному часі, який показав, що перспективним шляхом розвитку є використання нейромережевих методів для шифрування та дешифрування даних [10], [15], [22].

Аналіз публікацій [3], [5], [18] показує, що нейромережевий криптографічний захист даних переважно реалізується програмним шляхом. Основним недоліком такої реалізації є складність забезпечення режиму реального часу та обмежень, які висуваються до бортових систем, щодо маси, габаритів, енергоспоживання та вартості.

У роботах [3], [14], [24] розглянуто шляхи адаптації автоасоціативної нейронної мережі з неітераційним навчанням до задач криптографічного захисту даних. Особливістю функціонування такої нейромережі є можливість попереднього обчислення вагових коефіцієнтів і їх подальше використання під час шифрування та дешифрування даних. У роботі [25] показано, що для нейромережевого криптографічного шифрування та дешифрування даних використовуються ключі, до складу яких входять архітектура нейромережі та матриці вагових коефіцієнтів.

Аналіз робіт показує [1], [12], [13], [21], що для попереднього обчислення вагових коефіцієнтів застосовується метод головних компонент, який використовує систему власних векторів, які відповідають власним значенням коваріаційної матриці вхідних даних. У роботі [2] показано, що модель послідовних геометричних перетворень знаходиться в основі неітеративного методу навчання автоасоціативної нейронної мережі для операцій шифрування-дешифрування даних, для якої величини змінних, отримані внаслідок навчання мережі, перераховуються у відповідні вагові коефіцієнти міжнейронних зв'язків.

Отже, за результатами виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – вдосконалений метод нейромережевого шифрування (дешифрування) даних, який за рахунок розпаралелення процесу шифрування (дешифрування) та використання таблиць макрочасткових добутків забезпечує зменшення часу шифрування (дешифрування) при програмній реалізації, а також, розроблений метод адаптивного баркероподібного кодування / декодування, який за рахунок врахування співвідношенням сигнал/шум забезпечує високу завадостійкість та зменшує час передачі даних.

Практична значущість результатів дослідження – використання вдосконаленого методу нейромережевого шифрування (дешифрування) даних і розробленого методу адаптивного баркероподібного кодування / декодування забезпечує створення базових компонент системи нейромережевого захисту, баркероподібного кодування та передачі даних, адаптованих до використання у мобільних бортових системах.

Аналіз результатів тестування засобів нейромережевого шифрування (дешифрування) даних показує, що найбільш тривала операція – формування і навчання нейромережі, а час її виконання на мікрокомп'ютері стано-

вить біля 200 мс і не сильно залежить від архітектури обраної нейромережі. З іншої сторони, тривалість виконання процедур нейромережевого криптографічного шифрування та дешифрування блоків даних при реалізації на мікрокомп'ютері становить відповідно 30-38 мс та 23-35 мс. Отже, можна зробити висновок, що тривалість виконання процедур нейромережевого криптографічного шифрування та дешифрування блоків даних на базі мікрокомп'ютера є прийнятним для реалізації як вказаних задач, так і задач керування та моніторингу у режимі часу, близькому до реального.

Висновок / Conclusions

Запропоновано архітектуру системи нейромережевого захисту, баркероподібного кодування передачі даних, що ґрунтується на принципах змінного складу обладнання та модульності.

Описано процес розроблення базових компонентів системи нейромережевого захисту, кодування та передачі даних на основі інтегрованого підходу, який містить удосконалений метод нейромережевого шифрування та дешифрування даних і метод адаптивного баркероподібного кодування та декодування даних орієнтовані на сучасну елементну базу. Для розробки системи нейромережевого захисту, кодування та передачі даних обрано принципи: змінності складу обладнання; модульності; відкритості програмного забезпечення; спеціалізації та адаптації апаратно-програмних засобів до структури алгоритмів нейроподібного шифрування та дешифрування даних; програмної зміни архітектури нейромережі та розрядності баркероподібного коду. При цьому, задача розробки системи нейромережевого захисту з високими техніко-експлуатаційними характеристиками зводиться до мінімізації апаратних затрат при забезпеченні множини вимог і обмежень.

Вдосконалено метод нейромережевого шифрування (дешифрування) даних, який внаслідок розпаралелення процесу шифрування (дешифрування) та використання таблиць макрочасткових добутків забезпечує зменшення часу шифрування (дешифрування) при програмній реалізації. Розроблено метод адаптивного баркероподібного кодування / декодування, який внаслідок врахування співвідношенням сигнал/шум забезпечує високу завадостійкість та зменшує час передачі даних.

Описано створення апаратних засобів системи на основі розроблених базових компонентів нейромережевого захисту та баркероподібного кодування даних. З використанням апаратних і програмних засобів створеної системи визначено, що виконання операцій нейромережевого криптографічного шифрування та дешифрування блоків даних на базі мікрокомп'ютера здійснюється у часі, близькому до реального. Визначено експериментальним шляхом, що тривалість виконання шифрування та дешифрування блоків даних у цьому випадку становить відповідно 30-38 мс та 23-35 мс і не залежить істотно від обраної конфігурації нейроподібної мережі.

References

[1] Arvandi, M., Wu, S., Sadeghian, A., Melek, W. W., & Woungang, I. (2006). Symmetric cipher design using recurrent neural networks. Proceedings of the IEEE International Joint Conference on Neural Networks, 2039–2046.

[2] Chang, A. X. M., Martini, B., & Culurciello, E. (2015). Recurrent neural networks hardware implementation on FPGA: arXiv preprint arXiv:1511.05552.

[3] Chi, Zhang, Wei, Zou, Liping, Ma, & Zhiqing, Wang. (2020). Biologically inspired jumping robots: A comprehensive review, Robotics and Autonomous Systems, vol. 124.

[4] Corona-Bermúdez, E., Chimal-Eguía, J. C., & Téllez-Castillo, G. (2022). Cryptographic Services Based on Elementary and Chaotic Cellular Automata. *Electronics*, *11*(4), 613. https://doi.org/10.3390/electronics11040613

[5] Diamantaras, K. I., & Kung, S. Y. (1996). Principal Component Neural Networks. Theory and Applications (Wiley, 1996), 270 p.

[6] Haikin, S. (2016). Neural networks: full course (2nd ed . add. and revised). (Trans. from English). Moscow: Williams.

[7] Khan, S., Han, L., Lu, H., Butt, K., Bachira, G., & Khan, N. (2019). A New Hybrid Image Encryption Algorithm Based on 2D-CA, FSM-DNA Rule Generator, and FSBI. IEEE Access 2019, 7, 81333–81350. https://doi.org/10.1109/ACCESS.2019.2920383

[8] Korchenko, O., Tereykovsky, I., & Biloshchytsky, A. (2016). Methodology of development of neural network means of information security of Internet-oriented information systems. "Nash Format".

[9] Ostapov, S. (2013). Information security technologies. Kharkiv: KhNEU.

[10] Riznik, O. Ia., Tkachenko, R. O., & Kinash, Iu. Ye. (2019). Neiromerezheva tekhnologiia zakhistu ta peredachi danikh u realnomu chasi z vikoristanniam shumopodibnikh kodiv. Innovatciini tekhnologii u rozvitku suchasnogo suspilstva: zbirnik tez dopovidei mizhnarodnoi naukovo-praktichnoi konferentcii (Lviv, 18–19 kvitnia 2019 r.), 19–23. [In Ukrainian].

[11] Rudenko, O., & Bodyansky, E. (2006). Artificial neural networks. Kharkiv: SMIT Company Ltd.

[12] Sagar, V., & Kumar, K. (2014). A Symmetric Key Cryptographic Algorithm Using Counter Propagation Network (CPN). Proceedings of the 2014 ACM International Conference on Information and Communication Technology for Competitive Strategies. https://doi.org/10.1145/2677855.2677906

[13] Shihab, K. A. (2006). Backpropagation neural network for computer network security. *Journal of Computer Science*, vol. 2, no. 9, 710–715.

[14] Śledź, S., Ewertowski, M. W., & Piekarczyk, J. (2021). Applications of unmanned aerial vehicle (UAV) surveys and Structure from Motion photogrammetry in glacial and periglacial geomorphology. Geomorphology 2021, 378 p.

[15] Tcimbal, Iu. V. (2018). Neiromerezhevii metod simetrichnogo shifruvannia danikh. *Visnik Natcionalnogo universitetu "Lvivska politekhnika"*. Seriia: *Informatciini sistemi ta merezhi*, 901, 118–122. [In Ukrainian].

[16] Tereykovsky, I. (2007). Neural networks in the means of protection of computer information. Polygraph Consulting.

[17] Tkachenko, R., Tkachenko, P., Izonin, I., & Tsymbal, Y. (2018). Learning-based image scaling using neural-like structure of geometric transformation paradigm. Advances in Soft Computing and Machine Learning in Image Processing, Springer, 537–565. https://doi.org/10.1007/978-3-319-63754-9_25

[18] Tsmots, I. G., Rabik, V. G., & Lukashhuk, Iu. A. (2021). Rozroblennia mobilnikh zasobiv neiropodibnogo kriptografichnogo shifruvannia ta deshifruvannia danikh u realnomu chasi. Visnik Natcionalnogo universitetu "Lvivska politekhnika". Seriia: Informatciini sistemi ta merezhi, 9, 84–95. [In Ukrainian].

[19] Tsmots, I., Rabyk, V., Riznyk, O., & Kynash, Y. (2019). Method of Synthesis and Practical Realization of Quasi-Barker Codes. 2019 IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 76–79. https://doi.org/10.1109/STC-CSIT.2019.8929882

[20] Tsmots, I., Teslyuk, V., Teslyuk, T., Lukashchuk, Y. (2021). The method and simulation model of element base selection for protection system synthesis and data transmission. *International Journal of Sensors, Wireless Communications and Control, 11*(5), 518–530. https://doi.org/10.2174/2210327910999201022194630
[21] Tsmots, I., Tsymbal, Y., Khavalko, V., Skorokhoda, O., & Tesluyk, T. (2018). Neural-Like Means for Data Streams Encryption and Decryption in Real Time. Processing of the 2018 IEEE 2nd International Conference on Data Stream Mining and Processing, DSMP 2018, 438–443.
[22] Tsmots, I., Tsymbal, Yu., Skorokhoda, O., & Tkachenko, R. (2019). Neural-like Methods and Hardware Structures for Real-time Data Encryption and Decryption. Proceedings of 14th International Scientific and Technical Conference (CSIT), Lviv, Ukraine, 3. 248–253. https://doi.org/10.1109/STC-CSIT.2019.8929809
[23] Tsymbal, Yu. (2018). Neural network method of symmetric data encryption. Bulletin of the Lviv Polytechnic National University. Information systems and networks, 901, 118–122.
[24] Verma, A., & Ranga, V. (2020). Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review. IEEE Sens. J., 20, 5666–5690.
[25] Volna, E., Kotyrba, M., Kocian, V., & Janosek, M. (2012). Cryptography Based On Neural Network. Proceedings of the 26th European Conference on Modeling and Simulation, 386–391. https://doi.org/10.7148/2012-0386-0391
[26] Wang, M., Cong, S., & Zhang, S. (2018). Pseudo Chirp-Barker-Golay coded excitation in ultrasound imaging, 2018 Chinese Control And Decision Conference (CCDC), Shenyang, 4035–4039. https://doi.org/10.1109/CCDC.2018.8407824
[27] Wang, S., & He, P. (2018). Research on Low Intercepting Radar Waveform Based on LFM and Barker Code Composite Modulation, 2018 International Conference on Sensor Networks and Signal Processing (SNSP), Xian, China, 297–301. https://doi.org/10.1109/SNSP.2018.00064
[28] Zhou, K., Kang, Y., Huang, Y., & Feng, E. (2007). Encrypting Algorithm Based on RBF Neural Network. Proceedings of the IEEE Third International Conference on Natural Computation, 1, 765–768. https://doi.org/10.1109/ICNC.2007.353

I. G. Tsmots, Yu. V. Opotiak, O. Ya. Risnuk, O. M. Berezky, Yu. A. Lukashchuk
Lviv Polytechnic National University, Lviv, Ukraine

ARCHITECTURE AND IMPLEMENTATION OF BASIC COMPONENTS OF NEURAL NETWORK PROTECTION SYSTEM AND DATA TRANSMISSION CODING

The development of basic components of the neural network protection system, data transmission coding based on an integrated approach, which includes an improved method of neural network encryption (decryption) and the method of adaptive barker-like coding (decoding) of data, which focuses on modern element base. The principles of specialization and adaptation of hardware and software to the structure of algorithms for neuro-like encryption (decryption) of data, neural network architecture, and barker-like code are used to develop the system. The architecture of the system is proposed, which takes into account the variable composition of the equipment and modularity. The method of neural network encryption (decryption) of data has been improved. The time of neural network encryption and decryption of data depends on the size of the tables of macroparticle products. The size of the tables of pre-calculated macroparticle products is based on the provision of encryption and decryption of data in real-time. A method of adaptive barker-like encoding (decoding) has been developed, which, due to the signal-to-noise ratio, provides high noise immunity and reduces data transmission time. The hardware of the system, which was created using the developed basic components of neural network protection and barker-like data encoding, is described. When creating hardware, ready-made components and modules of industrial production are used as much as possible, and the availability of appropriate means of software code development is taken into account. Means of neural network cryptographic encryption (decryption) of data of the mobile part of the system are implemented using a microcomputer-based on SoC. Not the most powerful microcomputer of the NanoPi Duo type from FriendlyElec has been especially used to test the means of neural network cryptographic encryption (decryption) of data. Using the created system, it is determined that the performance of neural network cryptographic encryption (decryption) of data blocks based on a microcomputer is carried out in close to real-time. The time of formation and training of the neural network is about 200 ms, and the implementation of encryption and decryption procedures is about 35 ms and 30 ms, respectively, and does not depend significantly on the chosen configuration of the neural network.

Keywords: cryptographic protection; mobile system architecture; neural network encryption (decryption) method; adaptive barker-like encoding (decoding) method.

Інформація про авторів:

Цмоць Іван Григорович, д-р техн. наук, професор, кафедра автоматизованих систем управління. **Email:** ivan.tsmots@gmail.com; https://orcid.org/0000-0002-4033-8618

Опотяк Юрій Володимирович, канд. техн. наук, доцент, кафедра автоматизованих систем управління. **Email:** yurii.v.opotiak@lpnu.ua, https://orcid.org/0000-0001-9889-4177

Різник Олег Яремович, канд. техн. наук, доцент, кафедра інформаційних технологій видавничої справи. **Email:** oleh.y.riznyk@lpnu.ua; https://orcid.org/0000-0002-3815-043X

Березький Олег Миколайович, д-р техн. наук, професор, кафедра комп'ютерної інженерії ЗУНУ. **Email:** ilber62@gmail.com; https://orcid.org/0000-0001-9931-4154

Лукащук Юрій Андрійович, аспірант, кафедра автоматизованих систем управління. **Email:** urijlukas@gmail.com; https://orcid.org/0000-0002-8933-8635

Цитування за ДСТУ: Цмоць І. Г., Опотяк Ю. В., Різник О. Я., Березький О. М., Лукащук Ю. А. Архітектура та реалізація базових компонентів системи нейромережевого захисту і кодування передачі даних. *Український журнал інформаційних технологій.* 2022, т. 4, № 1. С. 53–62.

Citation APA: Tsmots, I. G., Opotiak, Yu. V., Risnuk, O. Ya., Berezky, O. M., & Lukashchuk, Yu. A. (2022). Architecture and implementation of basic components of neural network protection system and data transmission coding. *Ukrainian Journal of Information Technology, 4*(1), 53–62. https://doi.org/10.23939/ujit2022.01.053